EDHOC interop

LAKE, Interim, December 2020
Report from Interop #1

• 11th of December 9:00-11:00

• 2 implementations tested against each other: Timothy Claeys INRIA, Stefan Hristozov Fraunhofer AISEC

• Based on test vector on appendix B.1:
  • signature authentication and X.509 certificates
  • method = 0
  • selected cipher suite = 0
    (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)

• Successful in one direction, connection problems in the other direction

• Detailed notes: https://drive.google.com/drive/folders/1uHPYIiTKib9SQ74CXKtEPijiqWttCGu?usp=sharing
Next Steps

• Already good feedback about the test vectors to be incorporated
  • Both in the draft and in the github repo
  • Added a github issue: https://github.com/lake-wg/edhoc/issues/47

• More interop after the holidays: please state your preference!
  https://doodle.com/poll/mrhqqewzinegnmtq